

FIG.4

# LAYOUT OF PACKET IN WHICH TO TRANSMIT MAIN DATA

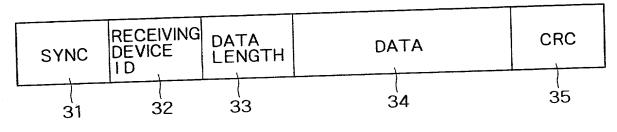


FIG.5

## LAYOUT OF PACKET IN WHICH TO TRANSMIT REQUEST DATA

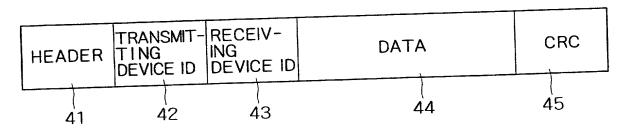
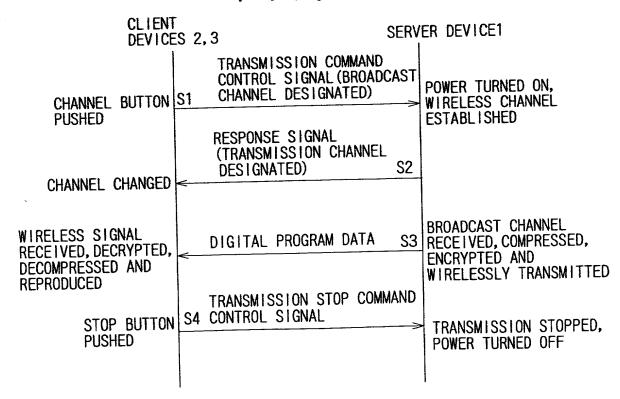


FIG.6

NETWORK	ON THE SAM (e.g., HOUS	ME NETWORK EHOLD)	NEIGHBORING NETWORK (e.g., NEXT-DOOR NEIGHBOR)
TECHNOLOGY	DEVICE ID=01	DEVICE ID=02	DEVICE ID=01
ENCRYPTION	DECRYPTABLE	DECRYPTABLE	NON- DECRYPTABLE
DEVICE ID	ONLY PACKETS HAVING THE OWN DEVICE ID OR PACKETS DESTINED FOR ALL DEVICES ARE RECEIVABLE	ONLY PACKETS HAVING THE OWN DEVICE ID OR PACKETS DESTINED FOR ALL DEVICES ARE RECEIVABLE	

#### FIG.7



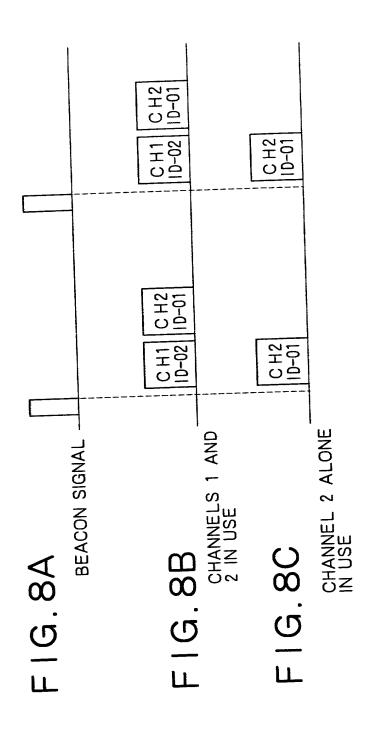
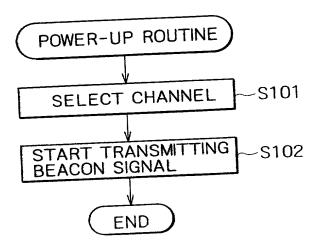
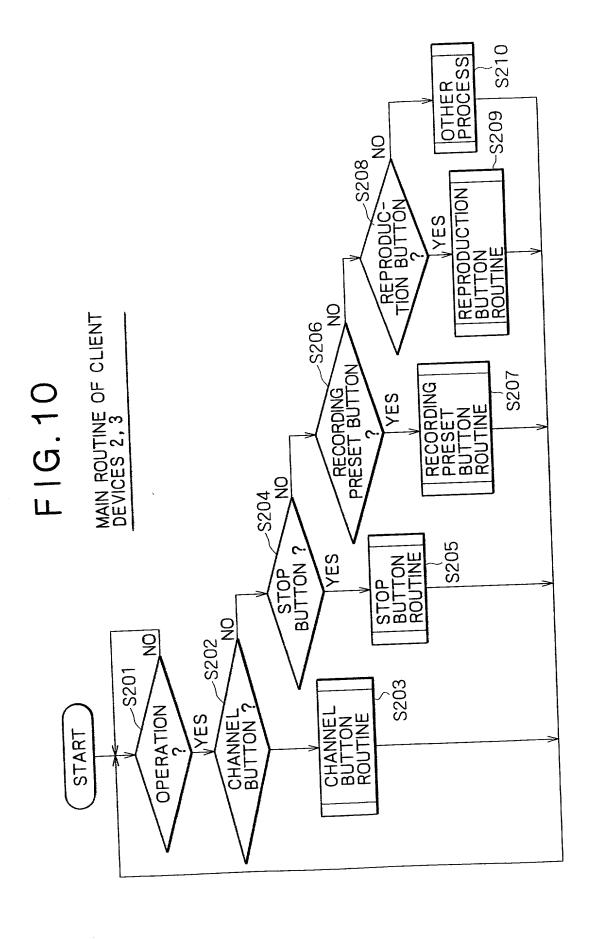
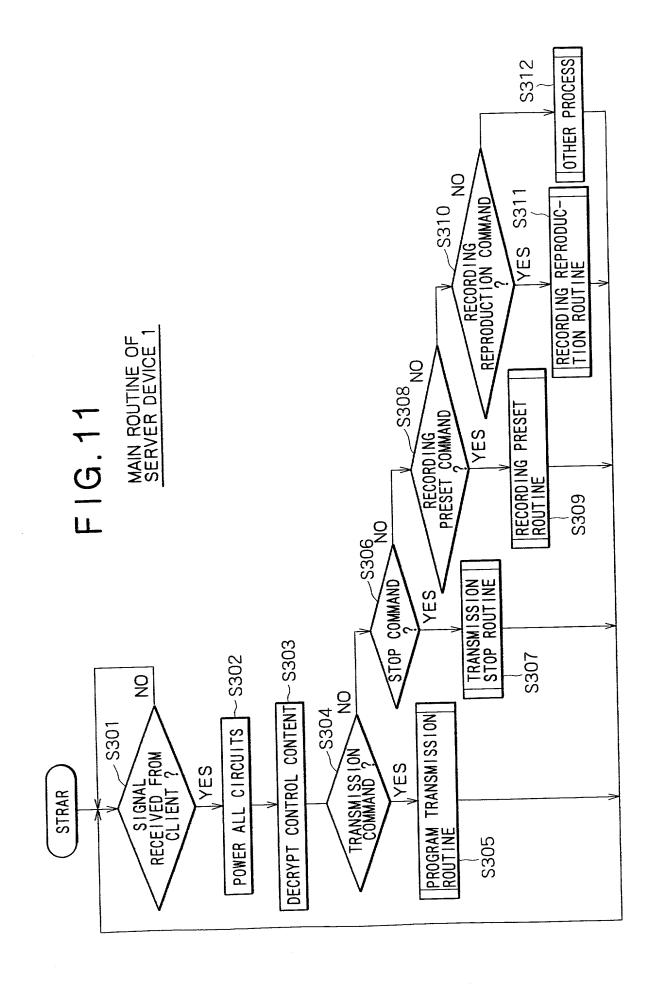


FIG.9

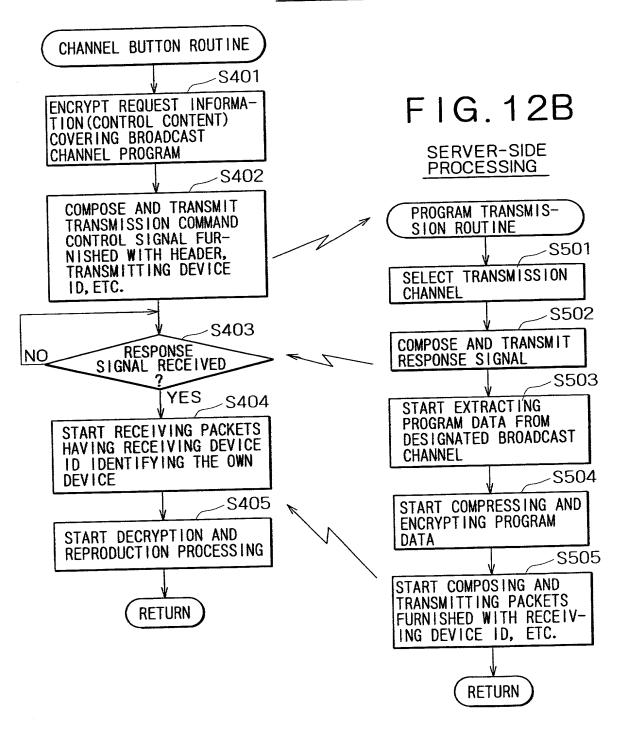


POWER UP PROCESSING OF SERVER DEVICE



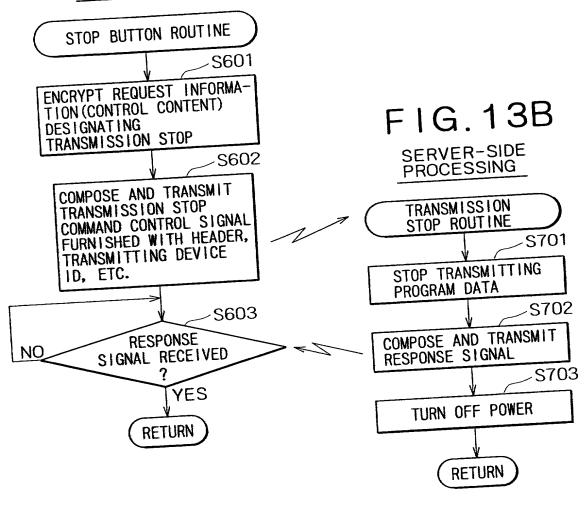


#### FIG. 12A CLIENT-SIDE PROCESSING

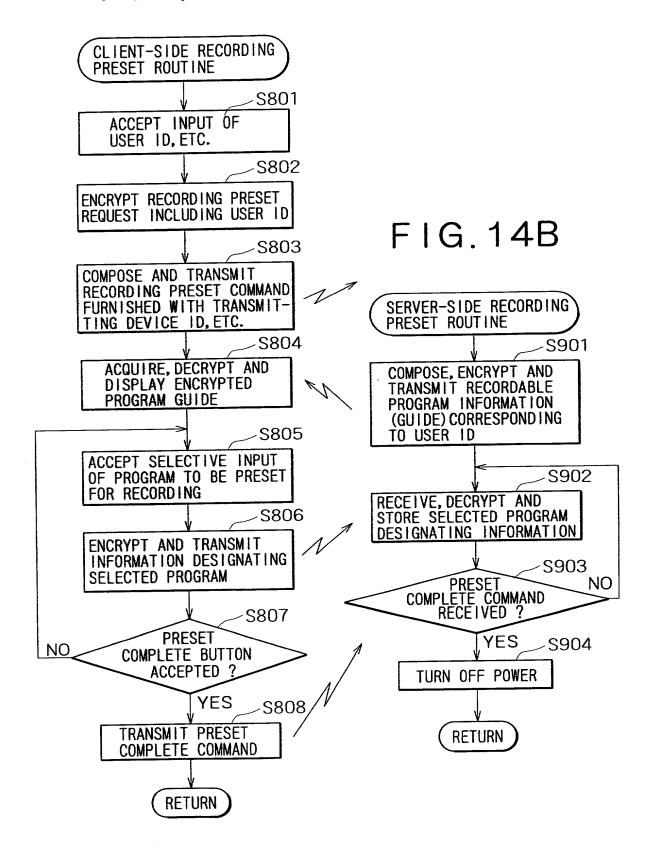


#### FIG. 13A

CLIENT-SIDE PROCESSING



#### FIG. 14A



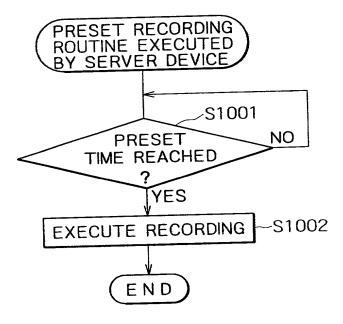
### FIG. 15

USER ID	RESTRICTIONS	DESCRIPTION
001	FREE	NO RESTRICTIONS
002	X(FOR ADULTS ONLY)	ADULTS-ONLY (X-RATED) PROGRAMS ARE UNAVAILABLE
003	X(FOR ADULTS ONLY)	ADULTS-ONLY (X-RATED) PROGRAM ARE UNAVAILABLE
	R (UNFIT FOR CHILDREN UNDER 16)	PROGRAMS RATED AS UNFIT FOR CHILDREN UNDER 16 (R-RATED) ARE UNAVAILABLE
	•	
	•	

F1G.16

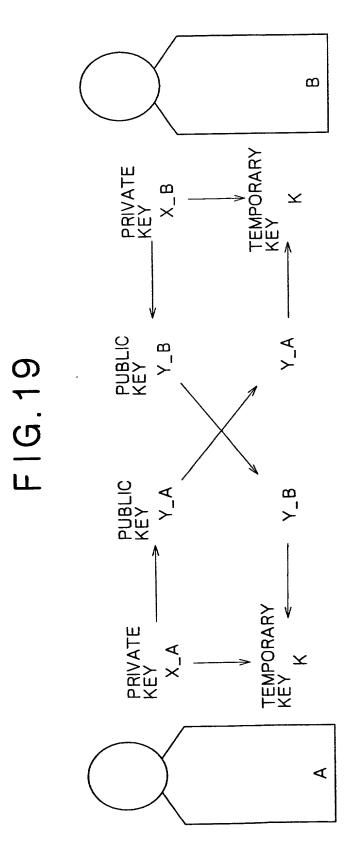
CAT I ON DEVICE	-	0	-	
CLASSIFICATION USER DEVICE	-	-	0	
F.	വ	&	7	
END	12:00, 8/25/2000	13:30, 8/25/2000	12:00, 8/25/2000	
START	11:00,	11:30,	11:00,	
USER ID	003	800	002	
PRESETTING DEVICE ID	10	02	01	
SEQ-	0 Z		ı m	

FIG. 17



#### FIG. 18A CLIENT-SIDE REPRODUCTION ROUTINE S1101 ACCEPT INPUT OF USER ID S1102 ENCRYPT REPRODUCTION FIG. 18B REQUEST INCLUDING USER ID S1103 SERVER-SIDE RE-COMPOSE AND TRANSMIT PRODUCTION ROUTINE REPRODUCTION COMMAND S1201 FURNISHED WITH TRANSMIT-TING DEVICE ID COMPOSE AND TRANSMIT S1104 RECORDING LIST INFORMA-TION CORRESPONDING ACQUIRE, DECRYPT AND DIS-TO USER ID PLAY ENCRYPTED RECORDING S1202 LIST INFORMATION RECEIVE AND DECRYPT S1105 INFORMATION DESIGNATING PROGRAM TO BE REPRODUCED ACCEPT SELECTIVE INPUT OF PROGRAM TO BE REPRODUCED S1203 -S1106 REPRODUC-NO ENCRYPT AND TRANSMIT TION EXECUTION COMMAND INFORMATION DESIGNATING RECEIVED 3 SELECTED PROGRAM S1204 YES -S1107 RETRIEVE. ENCRYPT AND REPRODUCTION NO TRANSMIT PROGRAM EXECUTION COMMAND ACCEPTED ? S1205 YES ~S1108 END OF NO **REPRODUCTION** TRANSMIT REPRODUCTION EXECUTION COMMAND YES -S1206 S1109 TURN OFF POWER START RECEIVING, DECRYP-TING AND REPRODUCING RECORDED PROGRAM RETURN

RETURN



# F1G.20

	ON DEVICE A SIDE	ON DEVICE B SIDE
PRIVATE KEY	X_A	X_B
PUBLIC KEY	Y_A=g^ (X_A)mod p	Y_B=g^ (X_B)mod p
TEMPORARY KEY	K=Y_B^(X_A)mod p =g^(X_A·X_B)mod p	K=Y_A^ (X_B)mod p =g^(X_B·X_A)mod p